PCT ORGANISATION MONDIALE DE LA PROPRIETE INTELLECTUELLE
Bureau international

DEMANDE INTERNATIONALE PUBLIEE EN VERTU DU TRAITE DE COOPERATION EN MATIERE DE BREVETS (PCT)

(51) Classification internationale des brevets 7 : G06F 1/00

A1

(11) Numéro de publication internationale: **WO 00/50977**

(43) Date de publication internationale: 31 août 2000 (31.08.00)

(21) Numéro de la demande internationale: PCT/FR00/00472

(22) Date de dépôt international: 25 février 2000 (25.02.00)

(30) Données relatives à la priorité:
99/02364 25 février 1999 (25.02.99) FR

(71) Déposant *(pour tous les Etats désignés sauf US)*: STMICROELECTRONICS S.A. [FR/FR]; 7, avenue Galliéni, F–94250 Gentilly (FR).

(72) Inventeur; et
(75) Inventeur/Déposant *(US seulement)*: ROMAIN, Fabrice [FR/FR]; Les Héliades Bâtiment A, 535, avenue de Bagatelle, F–13090 Aix–en–Provence (FR).

(74) Mandataire: BALLOT, Paul; Cabinet Ballot–Schmit, 7, rue Le Sueur, F–75116 Paris (FR).

(81) Etats désignés: JP, US, brevet européen (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE).

Publiée
Avec rapport de recherche internationale.
Avant l'expiration du délai prévu pour la modification des revendications, sera republiée si des modifications sont reçues.

(54) Title: ~~METHOD FOR MAKING SECURE A SEQUENCE OF OPERATIONS PERFORMED BY AN ELECTRONIC CIRCUIT IN~~ THE EXECUTION OF AN ALGORITHM

(54) Titre: PROCEDE DE SECURISATION D'UN ENCHAINEMENT D'OPERATIONS REALISEES PAR UN CIRCUIT ELECTRONIQUE DANS LE CADRE DE L'EXECUTION D'UN ALGORITHME

(57) Abstract

The invention concerns a method for making secure a sequence of working operations, of the same type, performed by an electronic circuit in the execution of an algorithm. The method is characterised in that it comprises a step which consists in introducing randomly one or several dummy operations in the sequence of operations, so as to prevent fraudulent access, by statistical analysis of electric currents, to protected data.

(57) Abrégé

L'invention concerne un procédé de sécurisation d'un enchaînement d'opérations utiles, de même type, réalisées par un circuit électronique dans le cadre de l'exécution d'un algorithme. Le procédé selon l'invention fait intervenir une étape consistant à introduire de façon aléatoire une ou plusieurs opérations factices dans l'enchaînement d'opérations, afin d'empêcher un accès frauduleux, par une analyse statistique de courants électriques, à des données protégées.

UNIQUEMENT A TITRE D'INFORMATION

Codes utilisés pour identifier les Etats parties au PCT, sur les pages de couverture des brochures publiant des demandes internationales en vertu du PCT.

AL	Albanie	ES	Espagne	LS	Lesotho	SI	Slovénie
AM	Arménie	FI	Finlande	LT	Lituanie	SK	Slovaquie
AT	Autriche	FR	France	LU	Luxembourg	SN	Sénégal
AU	Australie	GA	Gabon	LV	Lettonie	SZ	Swaziland
AZ	Azerbaïdjan	GB	Royaume-Uni	MC	Monaco	TD	Tchad
BA	Bosnie-Herzégovine	GE	Géorgie	MD	République de Moldova	TG	Togo
BB	Barbade	GH	Ghana	MG	Madagascar	TJ	Tadjikistan
BE	Belgique	GN	Guinée	MK	Ex-République yougoslave de Macédoine	TM	Turkménistan
BF	Burkina Faso	GR	Grèce			TR	Turquie
BG	Bulgarie	HU	Hongrie	ML	Mali	TT	Trinité-et-Tobago
BJ	Bénin	IE	Irlande	MN	Mongolie	UA	Ukraine
BR	Brésil	IL	Israël	MR	Mauritanie	UG	Ouganda
BY	Bélarus	IS	Islande	MW	Malawi	US	Etats-Unis d'Amérique
CA	Canada	IT	Italie	MX	Mexique	UZ	Ouzbékistan
CF	République centrafricaine	JP	Japon	NE	Niger	VN	Viet Nam
CG	Congo	KE	Kenya	NL	Pays-Bas	YU	Yougoslavie
CH	Suisse	KG	Kirghizistan	NO	Norvège	ZW	Zimbabwe
CI	Côte d'Ivoire	KP	République populaire démocratique de Corée	NZ	Nouvelle-Zélande		
CM	Cameroun			PL	Pologne		
CN	Chine	KR	République de Corée	PT	Portugal		
CU	Cuba	KZ	Kazakstan	RO	Roumanie		
CZ	République tchèque	LC	Sainte-Lucie	RU	Fédération de Russie		
DE	Allemagne	LI	Liechtenstein	SD	Soudan		
DK	Danemark	LK	Sri Lanka	SE	Suède		
EE	Estonie	LR	Libéria	SG	Singapour		

PROCEDE DE SECURISATION D'UN ENCHAINEMENT D'OPERATIONS REALISEES PAR UN CIRCUIT ELECTRONIQUE DANS LE CADRE DE L'EXECUTION D'UN ALGORITHME

La présente invention se rapporte à un procédé de sécurisation d'un enchaînement d'opérations réalisées par un circuit électronique dans le cadre de l'exécution d'un algorithme.

Plus particulièrement, l'invention concerne un procédé de sécurisation d'un enchaînement d'opérations utiles, de même type, réalisées par un circuit électronique dans le cadre de l'exécution d'un algorithme, la sécurisation étant apportée par la présence d'informations parasites qui gênent l'observation, depuis l'extérieur du circuit électronique, des manifestations physiques associées à l'exécution des opérations utiles.

Dans le cadre de l'invention, un algorithme doit être compris en tant qu'enchaînement d'actions nécessaires à l'accomplissement d'une tâche. Il ne s'agit par conséquent pas nécessairement de la mise en oeuvre d'un programme informatique.

Le domaine d'application de l'invention est essentiellement le domaine de la cryptologie. La cryptologie peut se définir comme étant la science de la dissimulation de l'information. Elle constitue, avec la sécurité physique des composants et des systèmes d'exploitation, la dimension essentielle de la sécurité des cartes à puces. La cryptologie englobe la cryptographie, qui est l'art de chiffrer et de déchiffrer des messages, et la cryptanalyse, qui est l'art de casser les codes secrets.

Dans les cartes à puce, la cryptographie met en oeuvre divers mécanismes qui ont pour but d'assurer soit la confidentialité des informations, soit

l'authentification des cartes ou des utilisateurs, soit encore la signature des messages.

L'ensemble des moyens mettant en oeuvre la cryptographie forme un crypto-système. De tels crypto-systèmes renferment des informations confidentielles, notamment pour chiffrer et déchiffrer des messages numériques.

Parmi ces informations confidentielles, on peut citer les clés de chiffrement et de déchiffrement, qui sont des paramètres d'une convention secrète utilisée pour le chiffrement et le déchiffrement de messages numériques.

L'utilisation de ces clés de chiffrement et de déchiffrement nécessite souvent plusieurs transferts des données les caractérisant. Lors de leur utilisation au sein d'un crypto-système, les données caractéristiques de clés numériques et d'autres informations confidentielles circulent entre différents registres et modules de mémoire ou de traitement. Ces transferts entre registres et/ou modules se traduisent par l'apparition de courants électriques ou de champs magnétiques porteurs d'informations confidentielles. Les informations confidentielles peuvent, par exemple, concerner des clés de chiffrement et de déchiffrement.

De tels crypto-systèmes posent un problème de visibilité depuis le monde extérieur. En effet, une mesure des signaux électriques ou des champs magnétiques nés des échanges d'informations entre différentes parties du circuit peut permettre d'accéder à des informations confidentielles qui participent à la protection de données par le système de chiffrement ou de déchiffrement.

Par exemple, un des signaux électriques peut se situer au niveau du plot d'alimentation du circuit, que ce dernier soit interne ou externe.

En effet, au moment de l'utilisation de la clé numérique par un composant habilité tel qu'une carte à puce, une certaine visibilité, par exemple sur la clé numérique, est rendue possible par l'étude de tels signaux électriques. Les signaux électriques sensibles peuvent être observés sur différents plots du circuit reliant notamment différents registres ou modules de mémoire ou de traitement.

Une clé numérique peut ainsi être découverte suite à une accumulation de mesures de signaux électriques ou magnétiques et à une étude statistique de ces mesures.

D'une façon plus générale, tout circuit électronique a une consommation électrique liée aux opérations qu'il effectue. Il est possible, en mesurant cette consommation, de découvrir des informations cachées dans le circuit. Ce problème se pose en tout composant sécurisé, et notamment les composants pour cartes à puce.

La découverte de données protégées par observation de courant nécessite en général une reproductibilité de la mesure de courant afin d'effectuer les traitements statistiques.

Ainsi, lorsqu'un circuit électronique exécute un algorithme contenant des opérations identiques ou voisines, et répétitives, telles que des transferts de données confidentielles entre registres, et où l'observation fine des opérations une par une peut révéler une information confidentielle, une analyse statistique fondée sur la mesure des courants électriques précédemment cités peut nuire à la sécurité du circuit électronique.

La présente invention a pour objet de pallier les problèmes qui viennent d'être décrits.

L'invention propose donc une méthode permettant de parer à une divulgation, par observation du courant, de données protégées.

A cet effet, l'invention propose un procédé de sécurisation d'un enchaînement d'opérations réalisées par un circuit électronique dans le cadre de l'exécution d'un algorithme qui assure la non-visibilité vis-à-vis d'une analyse des signaux électriques lors des transferts de données entre différents registres.

Pour atteindre ces objectifs, l'invention propose d'insérer des opérations factices dans un enchaînement d'opérations utiles, de même type, effectuées dans le cadre de l'exécution d'un algorithme. Les opérations factices sont très ressemblantes aux opérations utiles. Chaque opération factice est insérée à un rang aléatoire pour chaque exécution de l'algorithme. Ainsi, l'acquisition de mesures de courant comparables devient très difficile.

Une opération factice peut être conçue comme une opération présentant une signature identique ou très proche en pratique d'une opération utile en termes de paramètres physiques observables associés à l'exécution de cette instruction (consommation de courant, rayonnement magnétique, etc.). Ces paramètres physiques peuvent être notamment détectés au niveau d'un terminal d'alimentation en courant ou en tension du circuit.

De la sorte, les présentes opérations factices ne peuvent pas être détectées échantillon par échantillon, et donc empêchent ou du moins rendent très difficile une analyse statistique.

L'invention concerne donc un procédé de sécurisation d'un enchaînement d'opérations utiles, de même type, réalisées par un circuit électronique dans le cadre de l'exécution d'un algorithme, chacune des

opérations utiles correspondant à une étape de l'algorithme, caractérisé en ce que le procédé comprend l'étape consistant à introduire de façon aléatoire une ou plusieurs opérations factices, de même type, dans l'enchaînement d'opérations utiles.

Une opération factice du même type qu'une opération utile peut prendre différentes formes selon l'application en cours, dès lors qu'elle présente des caractéristiques physiques qui apparaissent identiques ou suffisamment proches d'une opération utile pour rendre sa détection difficile. A titre d'exemple non-limitatif, une opération factice peut être l'exécution réelle d'un calcul, mais sans enregistrement du résultat en mémoire, ou avec enregistrement, mais dans une mémoire inopérante pour l'opération considérée.

Les opérations factices permettent ainsi d'introduire de faux calculs, ou de faux sous-ensembles d'opérations.

La présente invention concerne également un dispositif électronique d'exécution d'un algorithme, par exemple une carte à puce, caractérisé en ce qu'il met en oeuvre le procédé de sécurisation précité, éventuellement avec les aspects optionnels qui sont décrits dans ce qui suit.

Les différents aspects et avantages de l'invention apparaîtront plus clairement dans la suite de la description, qui présente un exemple de mise en oeuvre préféré du procédé selon l'invention et qui n'est donné qu'à titre indicatif et nullement limitatif de l'invention.

Selon un mode préféré de l'invention, un certain nombre d'opérations factices sont insérées entre des opérations utiles, de même type, réalisées par un circuit électronique dans le cadre de l'exécution d'un algorithme. Ces opérations factices sont introduites de

façon aléatoire : ces opérations factices peuvent être introduites entre n'importe quelle opération utile associée à l'algorithme.

On peut également trouver une ou plusieurs opérations factices avant la première opération utile associée à un algorithme ou après la dernière opération utile associée à un algorithme. On peut également trouver plusieurs opérations factices consécutives.

Afin de donner des séries de mesure de courant différentes à chaque exécution d'un même algorithme, de nouveaux aléas sont introduits à chaque exécution d'un algorithme.

Néanmoins, dans une application préférée, le procédé selon l'invention comprend l'étape supplémentaire consistant à maintenir un écart de temps constant entre la réalisation de deux opérations, qu'elles soient utiles et/ou factices successives. Ainsi, l'insertion des opérations factices n'apparaît pas de façon évidente lors d'une étude temporelle des signaux électriques associés aux opérations utiles réalisées par un circuit électronique dans le cadre de l'exécution d'un algorithme.

Enfin, il est préférable, mais pas obligatoire, que le nombre d'opérations factices introduites dans l'enchaînement d'opérations utiles soit constant pour chaque nouvelle exécution de l'algorithme. Ainsi, le temps d'exécution de l'algorithme dans sa totalité est le même à chaque exécution de l'algorithme. Le fait que des opérations factices ont été introduites est ainsi invisible en première analyse, ce qui assure encore une meilleure sécurisation de l'enchaînement d'opérations utiles.

Selon l'invention, il est également possible de distribuer les aléas seulement sur certaines parties de l'algorithme. De plus, le procédé selon l'invention

peut également s'appliquer à des algorithmes dont les opérations sont ordonnées, c'est-à-dire que les opérations utiles doivent s'enchaîner dans un ordre qu'on ne peut pas changer.

Le nombre d'opérations factices introduites est, dans une application préférée de l'invention, de l'ordre de 2 pourcent sur le nombre total d'opérations effectuées.

REVENDICATIONS

1. Procédé de sécurisation d'un enchaînement d'opérations utiles, de même type, réalisées par un circuit électronique dans le cadre de l'exécution d'un algorithme, chacune des opérations utiles correspondant à une étape de l'algorithme, caractérisé en ce que le procédé comprend l'étape consistant à introduire de façon aléatoire une ou plusieurs opérations factices, de même type, dans l'enchaînement d'opérations.

2. Procédé de sécurisation d'un enchaînement d'opérations de même type selon la revendication 1, caractérisé en ce que le procédé comprend l'étape supplémentaire consistant à maintenir un écart de temps constant entre la réalisation de deux opérations utiles et/ou factices successives.

3. Procédé de sécurisation d'un enchaînement d'opérations de même type selon l'une des revendications 1 ou 2, caractérisé en ce que le nombre d'opérations factices introduites dans l'enchaînement d'opérations est constant pour chaque nouvelle exécution de l'algorithme.

4. Utilisation du procédé selon l'une des revendications précédentes dans le domaine de la cryptographie.

5. Dispositif électronique d'exécution d'un algorithme, caractérisé en ce qu'il met en oeuvre le procédé de sécurisation selon l'une quelconque des revendications 1 à 3.

6. Carte à puce comprenant un dispositif électronique d'exécution d'un algorithme, caractérisé en ce qu'il met en oeuvre le procédé de sécurisation selon l'une quelconque des revendications 1 à 3.

INTERNATIONAL SEARCH REPORT

Interr. ıal Application No
PCT/FR 00/00472

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 G06F1/00

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 7 G06F G07F H04L

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	WO 97 33217 A (UGON MICHEL ;BULL CP8 (FR)) 12 September 1997 (1997-09-12) abstract page 1, line 1 -page 2, line 21 page 3, line 11 - line 29	1,4,5
Y	---	6
X	EP 0 448 262 A (GEN INSTRUMENT CORP) 25 September 1991 (1991-09-25) column 1, line 1 -column 3, line 1 column 6, line 38 - line 52	1,5
A	---	2
Y	GB 2 319 705 A (MOTOROLA LTD) 27 May 1998 (1998-05-27) abstract; figure 1 page 3, line 8 - line 13 claims 1-8	6
	--- -/--	

[X] Further documents are listed in the continuation of box C.

[X] Patent family members are listed in annex.

° Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
9 June 2000	19/06/2000

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL – 2280 HV Rijswijk Tel. (+31–70) 340–2040, Tx. 31 651 epo nl, Fax: (+31–70) 340–3016	Powell, D

Form PCT/ISA/210 (second sheet) (July 1992)

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	COHEN F B: "OPERATING SYSTEM PROTECTION THROUGH PROGRAM EVOLUTION" COMPUTERS & SECURITY. INTERNATIONAL JOURNAL DEVOTED TO THE STUDY OF TECHNICAL AND FINANCIAL ASPECTS OF COMPUTER SECURITY,NL,ELSEVIER SCIENCE PUBLISHERS. AMSTERDAM, vol. 12, no. 6, page 565-584 XP000415701 ISSN: 0167-4048 page 568, left-hand column, paragraph 3 -page 569, right-hand column, paragraph 2 page 570, right-hand column, paragraph 3 page 571, right-hand column, paragraph 3 -page 572, left-hand column, paragraph 2 ---	2,3
A	DALLAS SEMICONDUCTOR CORP.: "SECTION 1: INTRODUCTION" 6 October 1993 (1993-10-06) , DATA BOOK SOFT MICROCONTROLLER, PAGE(S) 1-3,7,8,73,77-80,82,152-156,229,290-292 XP002053731 page 78 -----	2

INTERNATIONAL SEARCH REPORT

information on patent family members

Inter nal Application No
PCT/FR 00/00472

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
WO 9733217 A	12-09-1997	FR 2745924 A	12-09-1997
		AU 2031497 A	22-09-1997
		BR 9702118 A	26-01-1999
		CA 2221880 A	12-09-1997
		CN 1181823 A	13-05-1998
		EP 0826169 A	04-03-1998
		JP 10507561 T	21-07-1998
		NO 975116 A	06-01-1998
		US 5944833 A	31-08-1999
EP 0448262 A	25-09-1991	AT 152530 T	15-05-1997
		AU 637677 B	03-06-1993
		AU 7291591 A	26-09-1991
		CA 2037857 A	21-09-1991
		DE 69125881 D	05-06-1997
		DE 69125881 T	14-08-1997
		DK 448262 T	27-10-1997
		ES 2100207 T	16-06-1997
		GR 3023851 T	30-09-1997
		IE 74155 B	02-07-1997
		JP 4223530 A	13-08-1992
		US 5249294 A	28-09-1993
GB 2319705 A	27-05-1998	WO 9822878 A	28-05-1998
		EP 0938707 A	01-09-1999

RAPPORT DE RECHERCHE INTERNATIONALE

Demande Internationale No
PCT/FR 00/00472

A. CLASSEMENT DE L'OBJET DE LA DEMANDE
CIB 7 G06F1/00

Selon la classification internationale des brevets (CIB) ou à la fois selon la classification nationale et la CIB

B. DOMAINES SUR LESQUELS LA RECHERCHE A PORTE

Documentation minimale consultée (système de classification suivi des symboles de classement)
CIB 7 G06F G07F H04L

Documentation consultée autre que la documentation minimale dans la mesure où ces documents relèvent des domaines sur lesquels a porté la recherche

Base de données électronique consultée au cours de la recherche internationale (nom de la base de données, et si réalisable, termes de recherche utilisés)

C. DOCUMENTS CONSIDERES COMME PERTINENTS

Catégorie °	Identification des documents cités, avec, le cas échéant, l'indication des passages pertinents	no. des revendications visées
X	WO 97 33217 A (UGON MICHEL ;BULL CP8 (FR)) 12 septembre 1997 (1997-09-12) abrégé page 1, ligne 1 -page 2, ligne 21 page 3, ligne 11 - ligne 29	1,4,5
Y	---	6
X	EP 0 448 262 A (GEN INSTRUMENT CORP) 25 septembre 1991 (1991-09-25) colonne 1, ligne 1 -colonne 3, ligne 1 colonne 6, ligne 38 - ligne 52	1,5
A	---	2
Y	GB 2 319 705 A (MOTOROLA LTD) 27 mai 1998 (1998-05-27) abrégé; figure 1 page 3, ligne 8 - ligne 13 revendications 1-8	6
	--- -/--	

[X] Voir la suite du cadre C pour la fin de la liste des documents

[X] Les documents de familles de brevets sont indiqués en annexe

° Catégories spéciales de documents cités:

"A" document définissant l'état général de la technique, non considéré comme particulièrement pertinent

"E" document antérieur, mais publié à la date de dépôt international ou après cette date

"L" document pouvant jeter un doute sur une revendication de priorité ou cité pour déterminer la date de publication d'une autre citation ou pour une raison spéciale (telle qu'indiquée)

"O" document se référant à une divulgation orale, à un usage, à une exposition ou tous autres moyens

"P" document publié avant la date de dépôt international, mais postérieurement à la date de priorité revendiquée

"T" document ultérieur publié après la date de dépôt international ou la date de priorité et n'appartenenant pas à l'état de la technique pertinent, mais cité pour comprendre le principe ou la théorie constituant la base de l'invention

"X" document particulièrement pertinent; l'invention revendiquée ne peut être considérée comme nouvelle ou comme impliquant une activité inventive par rapport au document considéré isolément

"Y" document particulièrement pertinent; l'invention revendiquée ne peut être considérée comme impliquant une activité inventive lorsque le document est associé à un ou plusieurs autres documents de même nature, cette combinaison étant évidente pour une personne du métier

"&" document qui fait partie de la même famille de brevets

Date à laquelle la recherche internationale a été effectivement achevée	Date d'expédition du présent rapport de recherche internationale
9 juin 2000	19/06/2000

Nom et adresse postale de l'administration chargée de la recherche internationale	Fonctionnaire autorisé
Office Européen des Brevets, P.B. 5818 Patentlaan 2 NL – 2280 HV Rijswijk Tel. (+31–70) 340–2040, Tx. 31 651 epo nl, Fax: (+31–70) 340–3016	Powell, D

1

Formulaire PCT/ISA/210 (deuxième feuille) (juillet 1992)

RAPPORT DE RECHERCHE INTERNATIONALE

Renseignements relatifs aux membres de familles de brevets

Dem. internationale No
PCT/FR 00/00472

Document brevet cité au rapport de recherche	Date de publication	Membre(s) de la famille de brevet(s)	Date de publication
WO 9733217 A	12-09-1997	FR 2745924 A	12-09-1997
		AU 2031497 A	22-09-1997
		BR 9702118 A	26-01-1999
		CA 2221880 A	12-09-1997
		CN 1181823 A	13-05-1998
		EP 0826169 A	04-03-1998
		JP 10507561 T	21-07-1998
		NO 975116 A	06-01-1998
		US 5944833 A	31-08-1999
EP 0448262 A	25-09-1991	AT 152530 T	15-05-1997
		AU 637677 B	03-06-1993
		AU 7291591 A	26-09-1991
		CA 2037857 A	21-09-1991
		DE 69125881 D	05-06-1997
		DE 69125881 T	14-08-1997
		DK 448262 T	27-10-1997
		ES 2100207 T	16-06-1997
		GR 3023851 T	30-09-1997
		IE 74155 B	02-07-1997
		JP 4223530 A	13-08-1992
		US 5249294 A	28-09-1993
GB 2319705 A	27-05-1998	WO 9822878 A	28-05-1998
		EP 0938707 A	01-09-1999

C.(suite) DOCUMENTS CONSIDERES COMME PERTINENTS

Catégorie	Identification des documents cités, avec, le cas échéant, l'indicationdes passages pertinents	no. des revendications visées
A	COHEN F B: "OPERATING SYSTEM PROTECTION THROUGH PROGRAM EVOLUTION" COMPUTERS & SECURITY. INTERNATIONAL JOURNAL DEVOTED TO THE STUDY OF TECHNICAL AND FINANCIAL ASPECTS OF COMPUTER SECURITY,NL,ELSEVIER SCIENCE PUBLISHERS. AMSTERDAM, vol. 12, no. 6, page 565-584 XP000415701 ISSN: 0167-4048 page 568, colonne de gauche, alinéa 3 -page 569, colonne de droite, alinéa 2 page 570, colonne de droite, alinéa 3 page 571, colonne de droite, alinéa 3 -page 572, colonne de gauche, alinéa 2 ---	2,3
A	DALLAS SEMICONDUCTOR CORP.: "SECTION 1: INTRODUCTION" 6 octobre 1993 (1993-10-06) , DATA BOOK SOFT MICROCONTROLLER, PAGE(S) 1-3,7,8,73,77-80,82,152-156,229,290-292 XP002053731 page 78 -----	2

DOCKET NO: P2001,0023
SERIAL NO: _____
APPLICANT: Hermo Hartliebdal.

LERNER AND GREENBERG P.A.
P.O. BOX 2480
HOLLYWOOD, FLORIDA 33022
TEL. (954) 925-1100